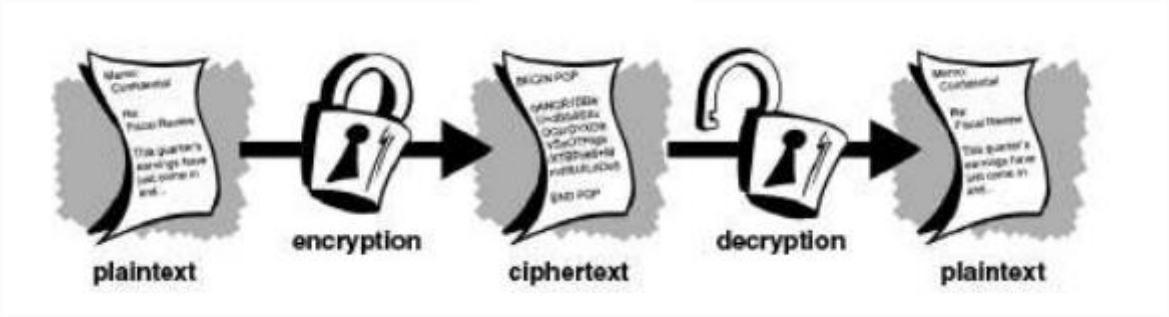
Introduction to PGP



(Note- GPA has been shown to not be very secure- whatever that means, given we're talking PGP encryption here. This example is only used as it is a simple program and thus teaches the basics which the reader is expected to build their knowledge upon.. A more secure option would be GPG4USB: http://www.gpg4usb.org/)

A popular and useful method of encryption is known as public key, or *asymmetric key cryptography.*

This method is based on two '**keys**': public and private. You have a private key which you keep stored securely, and your public key you give to someone so they can contact you via the encrypted method provided by the asymmetric encryption procedure.

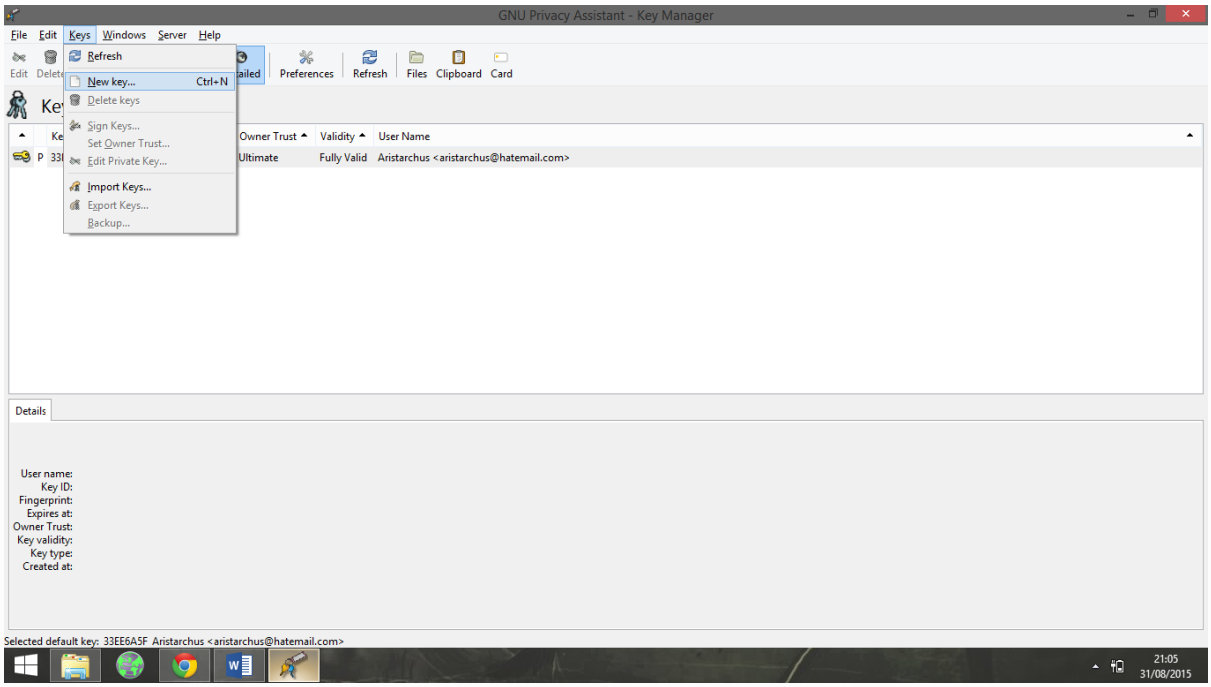
It is similar to having a normal key which only you possess, and a series of padlocks. You can give out these padlocks, which people can use to lock cases to send you securely- but only you can open them, as only you have the private key. The private/secret key has the algorithm for which the public key was encrypted. Without the private key, it is jargon and impossible to decipher.

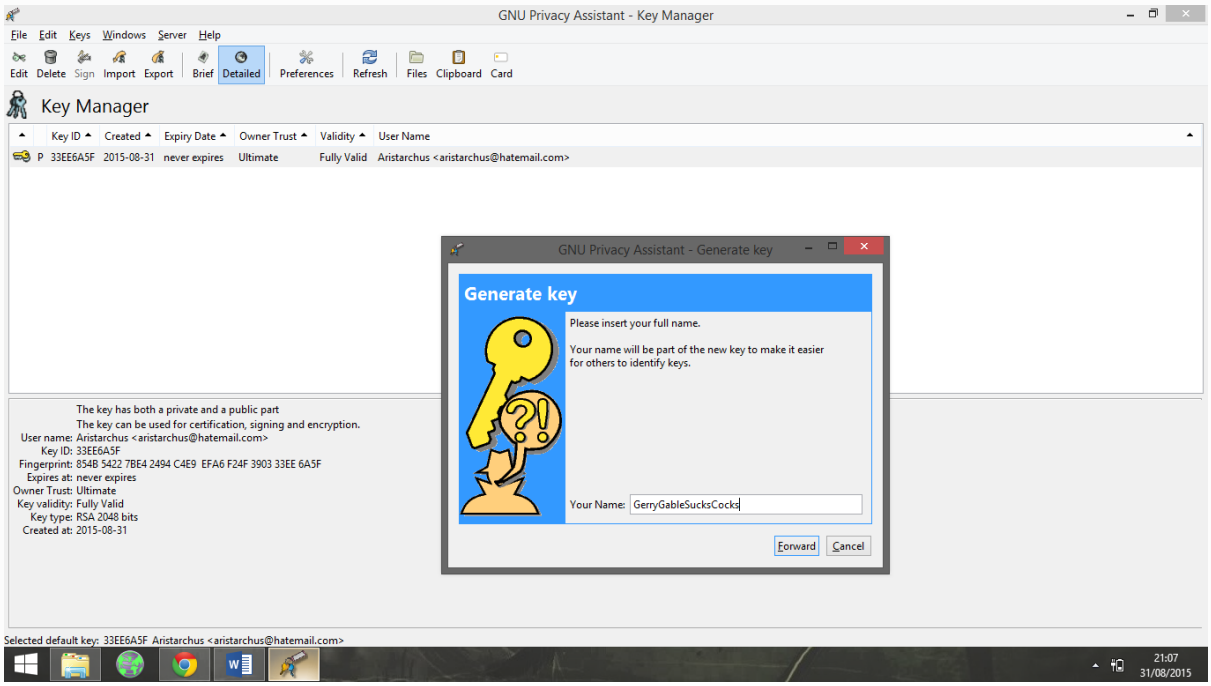
Step 1

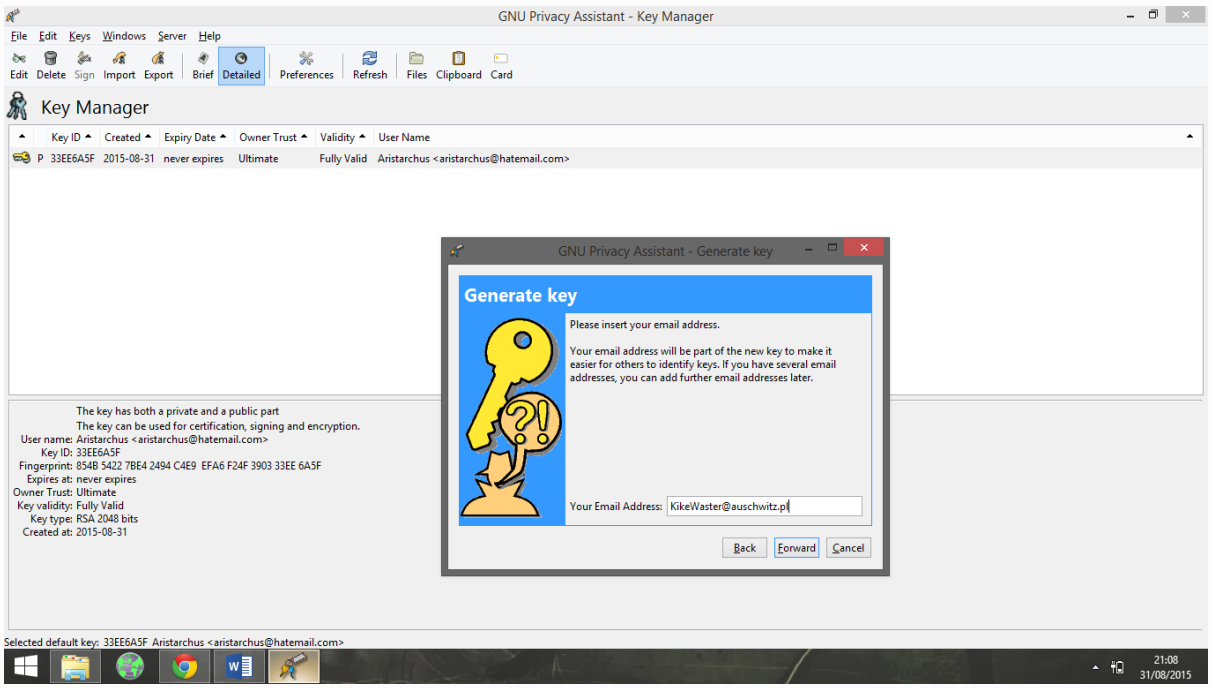
Get a PGP program- a popular one is GPA: http://gpg4win.org/download.html

When installing gpg4win you get the option to install which programs you want from the package. By default, GPA is not checked. Be sure to check GPA.

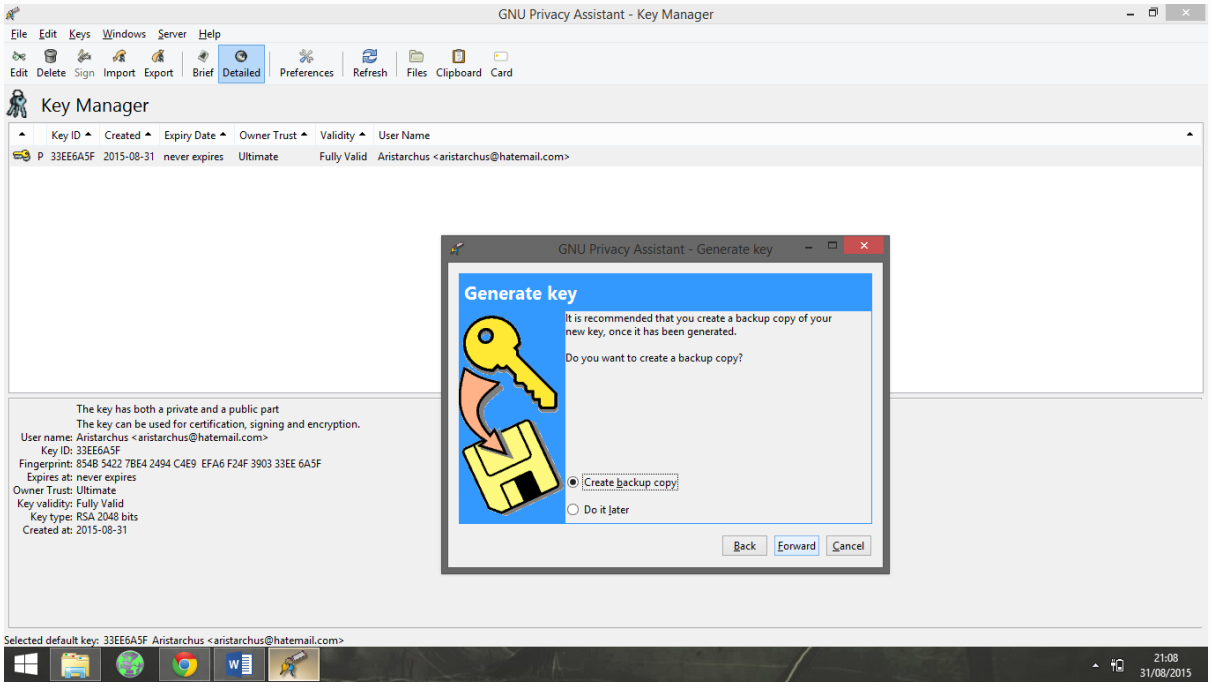
Now we need to make a PGP key. Don't input real info, obviously.



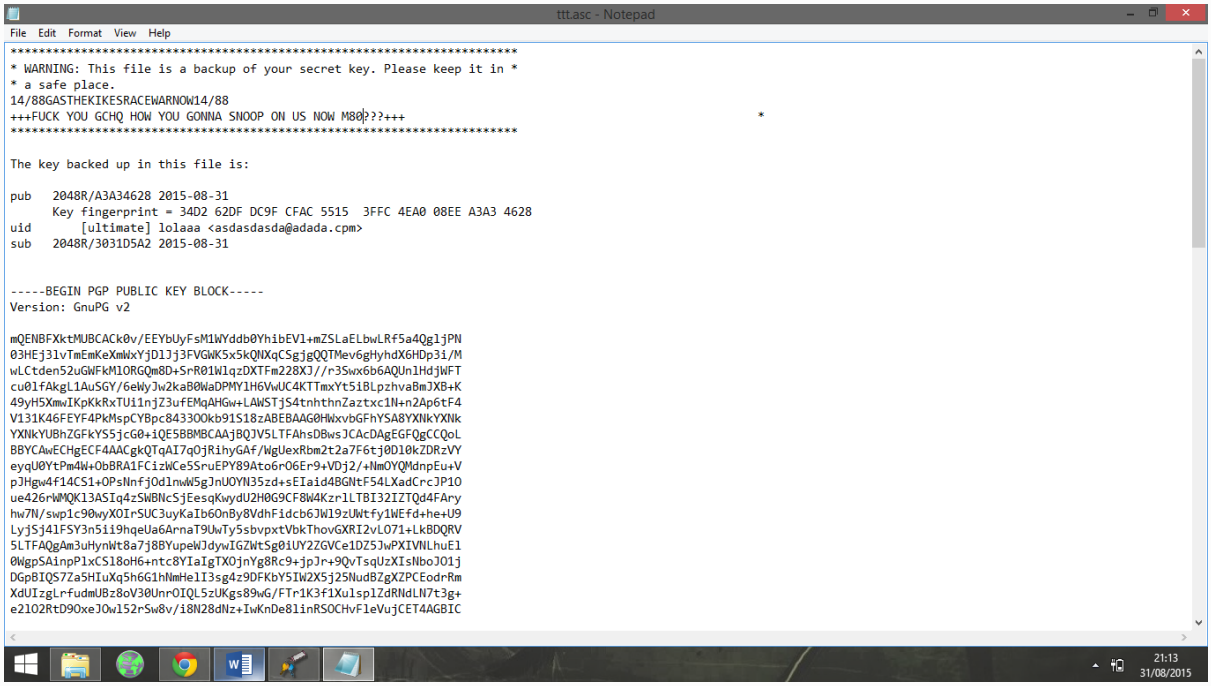

GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Created Expiry Date Owner Trust Validity User Name
P 33EE6A5F 2015-08-31 never expires Ultimate Fully Valid Aristarchus <aristarchus@hatemail.com>
GNU Privacy Assistant - Generate key
Generate key
Please insert your full name.
Your name will be part of the new key to make it easier for others to identify keys.
Your Name: GerryGableSucksCocks
Forward Cancel
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: Aristarchus <aristarchus@hatemail.com>
Key ID: 33EE6A5F
Fingerprint: 854B 5422 7BE4 2494 C4E9 EFA6 F24F 3903 33EE 6A5F
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2015-08-31
Selected default key: 33EE6A5F Aristarchus <aristarchus@hatemail.com>
21:07
31/08/2015


GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Created Expiry Date Owner Trust Validity User Name
P 33EE6A5F 2015-08-31 never expires Ultimate Fully Valid Aristarchus <aristarchus@hatemail.com>
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: Aristarchus <aristarchus@hatemail.com>
Key ID: 33EE6A5F
Fingerprint: 854B 5422 7BE4 2494 C4E9 EFA6 F24F 3903 33EE 6A5F
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2015-08-31
GNU Privacy Assistant - Generate key
Generate key
Please insert your email address.
Your email address will be part of the new key to make it easier for others to identify keys. If you have several email addresses, you can add further email addresses later.
Your Email Address: KikeWaster@auschwitz.pl
Back Forward Cancel
Selected default key: 33EE6A5F Aristarchus <aristarchus@hatemail.com>
21:08
31/08/2015

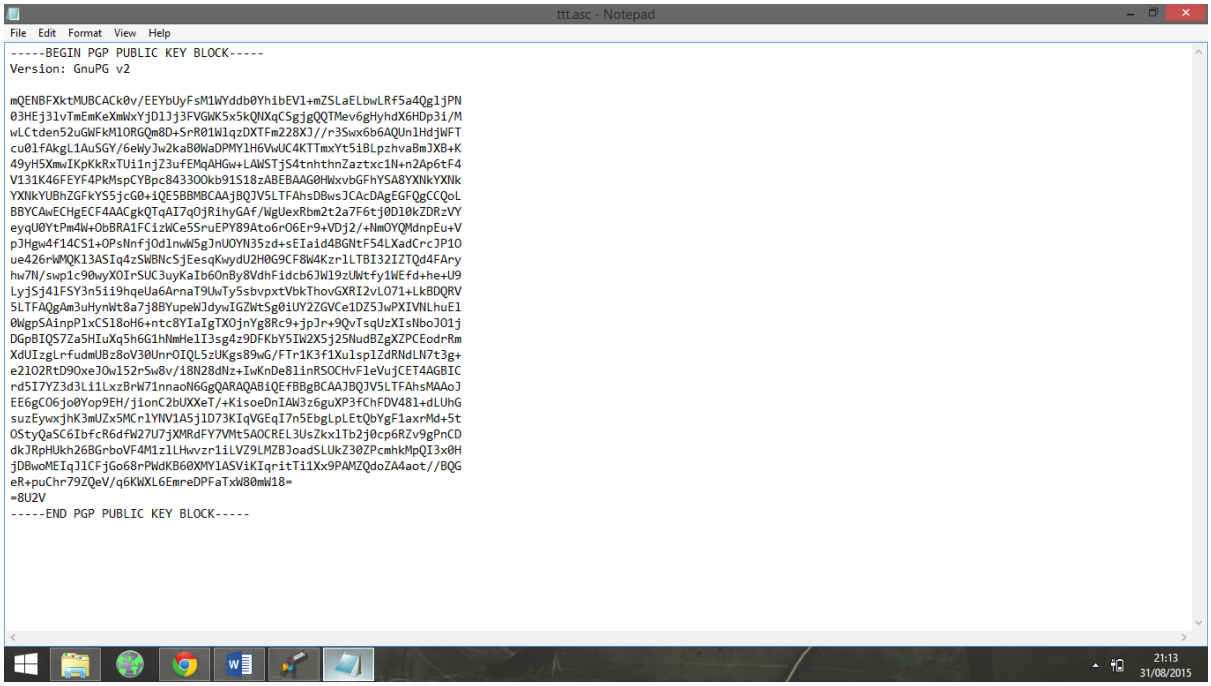
You will now be asked to make a backup copy of your key. Do so. This is where your public key will be that you give to others to contact you. Make a secure passphrase- DON'T FORGET IT. Be sure to give it a unique name, as it default names it the file directory (e.g. MyDocuments/SecretNaziStuff/asc.) and thus doesn't show up. So name it 'Public Key' or something similar.


GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Created Expiry Date Owner Trust Validity User Name
P 33EE6A5F 2015-08-31 never expires Ultimate Fully Valid Aristarchus <aristarchus@hatemail.com>
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: Aristarchus <aristarchus@hatemail.com>
Key ID: 33EE6A5F
Fingerprint: 854B 5422 7BE4 2494 C4E9 EFA6 F24F 3903 33EE 6A5F
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2015-08-31
GNU Privacy Assistant - Generate key
Generate key
It is recommended that you create a backup copy of your new key, once it has been generated.
Do you want to create a backup copy?
Create backup copy
Do it later
Back Forward Cancel
Selected default key: 33EE6A5F Aristarchus <aristarchus@hatemail.com>
21:08
31/08/2015

Find where you put the back up of your key. It will be an .asc file. Open it using Notepad, and you will see the following:

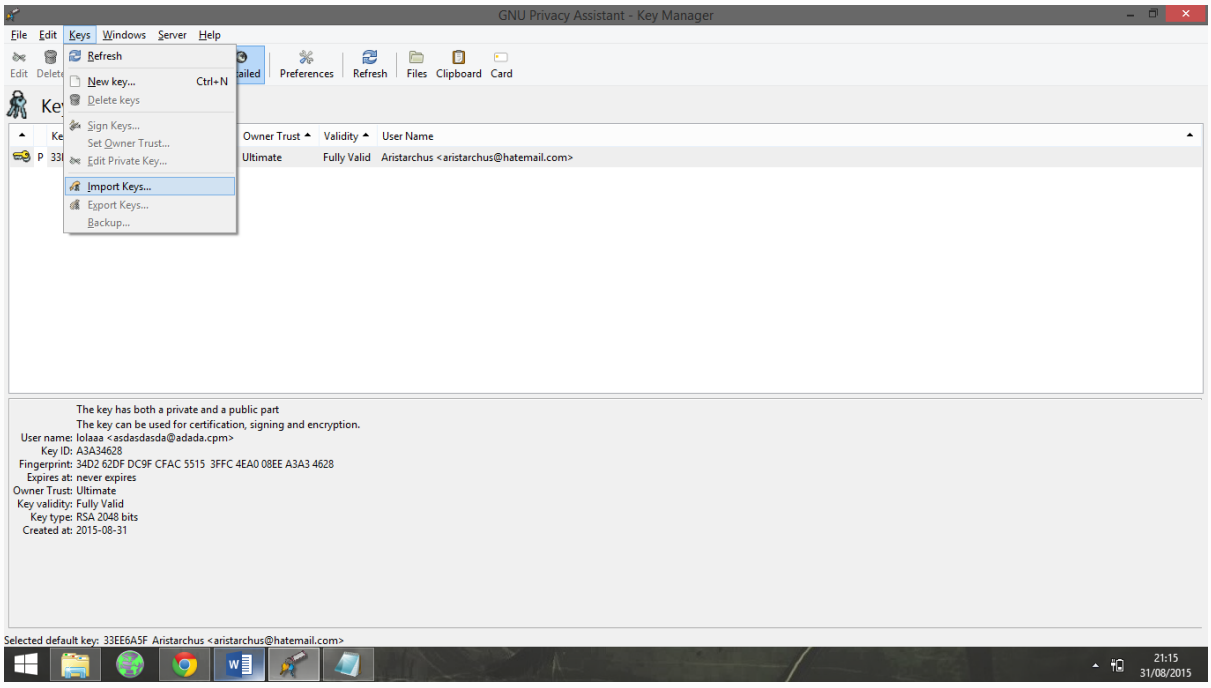


When sharing your key with others, copy and paste from the beginning dashes to the end dashes. Be sure to keep this .asc file somewhere secure as it has your private key on it also. A usb stick you won't lose or somewhere like an encrypted folder is just two ideas. I keep mine in my ipod's files.



To obtain someone else's public key, simply open a notepad file, copy and paste their key and save the text file.

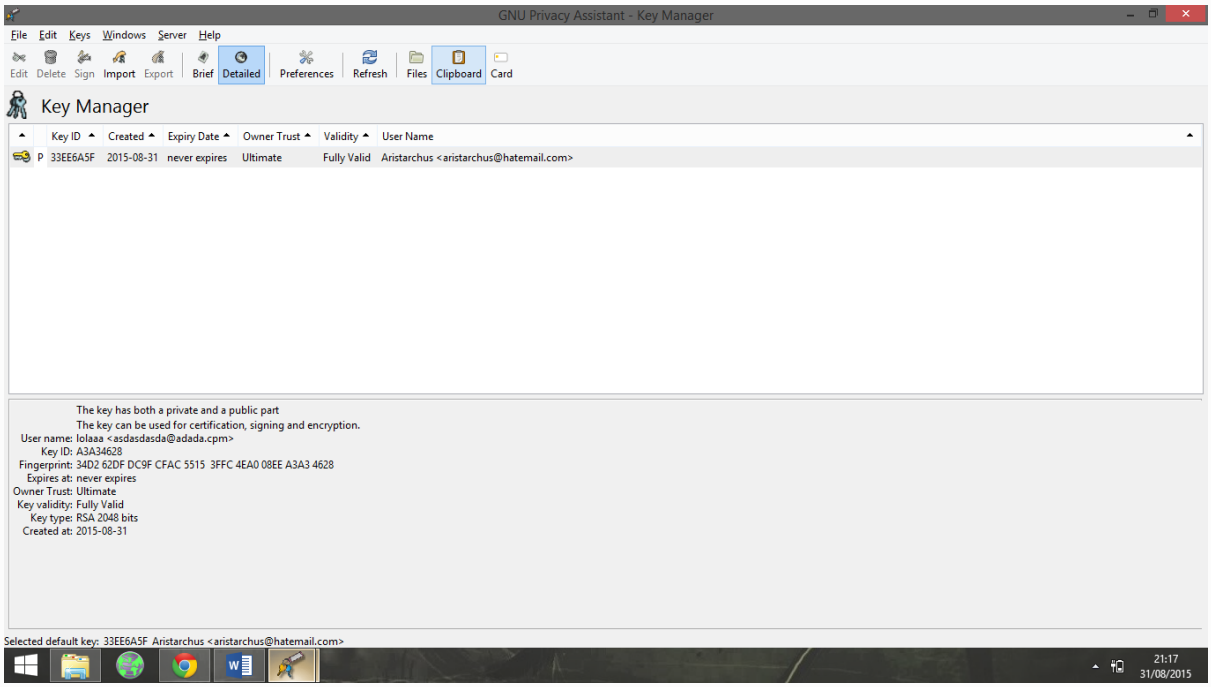
Now, go to your GPA program and in the Keys menu where you made your key, select import keys.



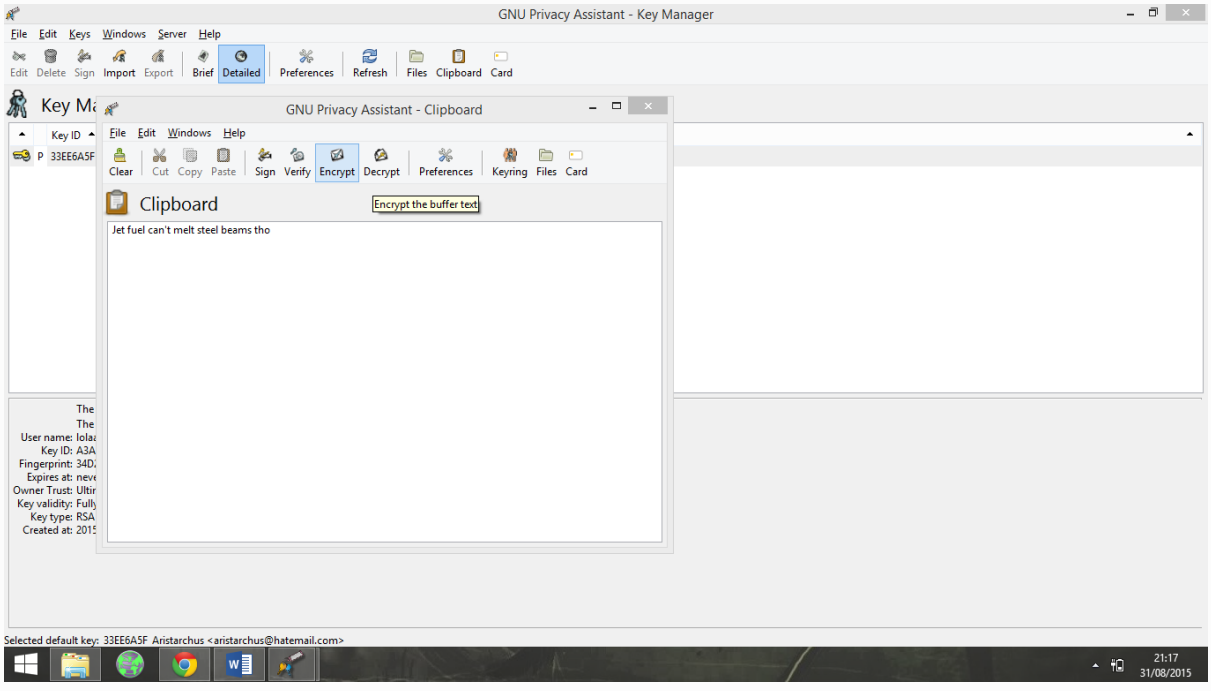
Select the Text file you saved with the public key in it. If successful, a notice will appear telling you so

Step 2- Sending an encrypted message

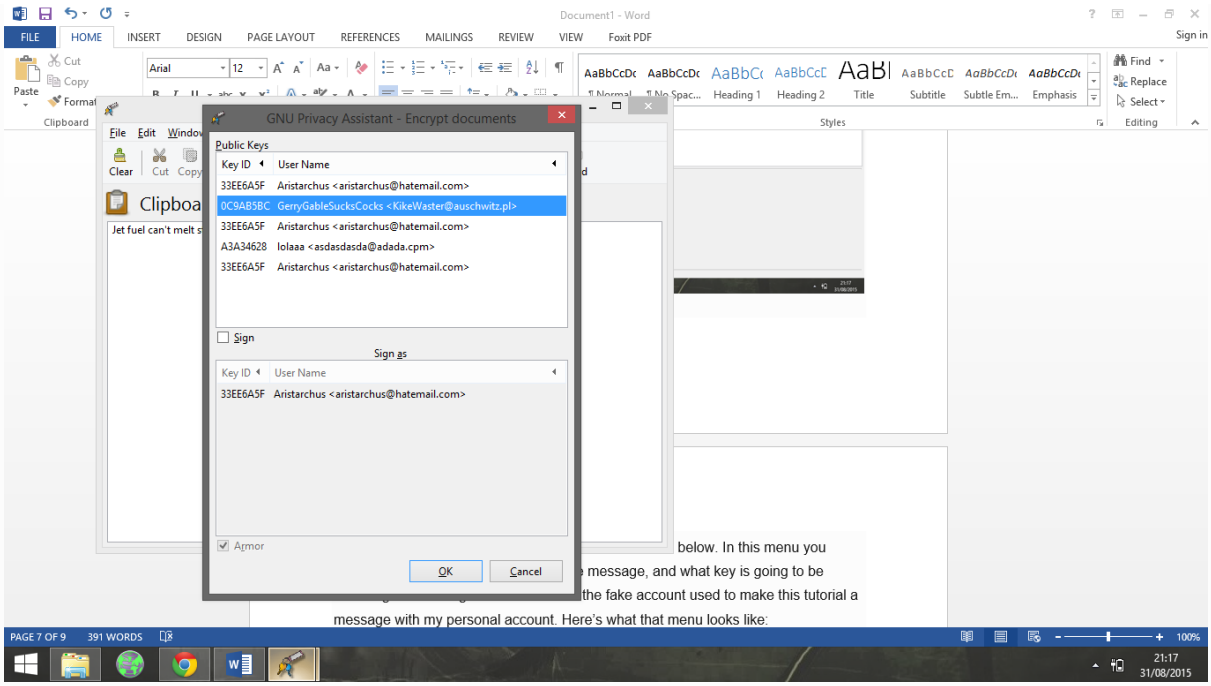
Open the clipboard and type your message, and select encrypt to encrypt it.


GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Created Expiry Date Owner Trust Validity User Name
P 33EE6A5F 2015-08-31 never expires Ultimate Fully Valid Aristarchus <aristarchus@hatemail.com>
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: lolaaa <asdasdasda@adada.cpm>
Key ID: A3A34628
Fingerprint: 34D2 62DF DC9F CFAC 5515 3FFC 4EA0 08EE A3A3 4628
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2015-08-31
Selected default key: 33EE6A5F Aristarchus <aristarchus@hatemail.com>
21:17
31/08/2015

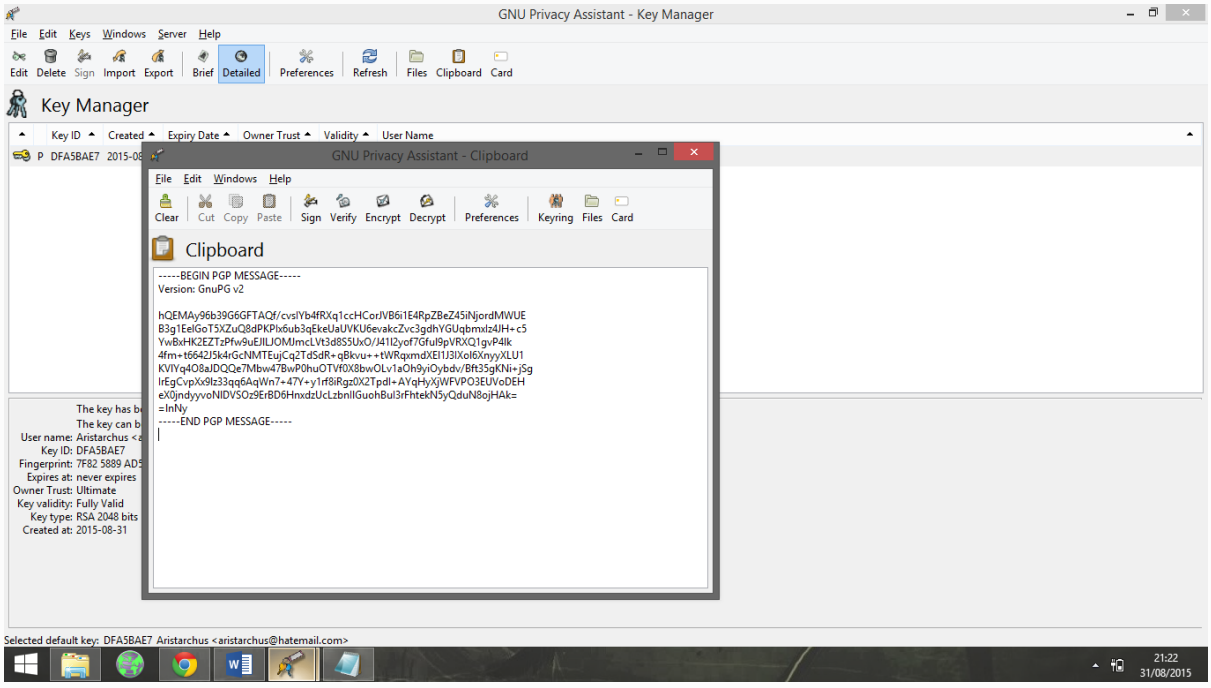
Now type in the message you want to send, and click ‘encrypt’.


GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
GNU Privacy Assistant - Clipboard
File Edit Windows Help
Clear Cut Copy Paste Sign Verify Encrypt Decrypt Preferences Keyring Files Card
Clipboard
Encrypt the buffer text
Jet fuel can't melt steel beams tho
Selected default key: 33EE6A5F Aristarchus <aristarchus@hatemail.com>
21:17
31/08/2015

You are asked to select which key to use to encrypt the message



You will then end up with an encrypted message which looks something like this:



This is the encrypted message you send in place of normal text (cleartext).It is a very useful tool to hide in plain sight, as only those who possess the keys can decrypt it (unless you've given your public key out- but, you can always make another one). To decrypt a PGP message, simply paste it into your PGP program clipboard and click 'decrypt'.

Further info: https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp